REMARKS

Figure 1 has been amended to illustrate processor(s) 31, RAM 32, operating system 33, ROM 34, bus 35 and disk storage device 36 in computer 12. Support is found from the statement "Honeypot 12 can be a server, workstation, embedded device such as a Single Board Computer (SBC)" on Page 7 lines 10-11 and the well known and inherent architecture of a computer to include these components.

> "MPEP 2163.07(a) Inherent Function, Theory, or Advantage
>
> By disclosing in a patent application a device that inherently performs a function or has a property, operates according to a theory or has an advantage, a patent application necessarily discloses that function, theory or advantage, even though it says nothing explicit concerning it. The application may later be amended to recite the function, theory or advantage without introducing prohibited new matter. *In re Reynolds*, 443 F.2d 384, 170 USPQ 94 (CCPA 1971); *In re Smythe*, 480 F. 2d 1376, 178 USPQ 279 (CCPA 1973). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted)."

No new matter has been added.

Figure 1 has also been amended to change the legend in box 30 from "Tool" to "Packet Filtering Program". This complies with the name of the program 30 as used throughout the patent application including Page 7 lines 25-26. No new matter has been added.

The Specification has also been amended to state, "Program 30 is stored in disk storage device 36 for execution by one or more processors 31 via RAM 32." Support is found on Page 7 lines 25-26 which states, "Honeypot includes a honeypot packet filtering program 30 …" and subsequent pages and Figure 2 which explain the operation of program 30. Support is also found from the well known manner of installation and execution of a program within a computer. See MPEP 2163.07(a) Inherent Function, Theory, or Advantage, quoted above. No new matter has been added.

The claims were amended to delete "or portion thereof" after "a known exploit". This was done to avoid confusion with "OR" used for other alternative language in the fourth program instructions, and to avoid confusion with "AND" used in the fifth program instructions. This deletion of "or portion thereof" was **not** made to distinguish prior art. New claims 25-28 have been added.

Claims 1-2, 4-5, 7, 12 and 21-22 were rejected under 35 USC 103(b) based on US Patent Publication 2003/0145228 to Suuronen et al. and US Patent Publication 2002/0116512 to Amit et al. The Board affirmed this rejection based on a misunderstanding of the scope of the fifth element of the independent claims (as it was phrased before this Amendment). The fifth program instructions, as phrased before this Amendment, stated "fifth program instructions, responsive to said packet **not being** a known exploit or portion thereof, addressed to a broadcast IP address of a network, network administration traffic or another type of traffic known to be benign, to determine and report that said packet is a new, exploit candidate". The Board stated, "We note that the fourth and fifth program instructions are claimed in the alternative and, therefore, Suuronen's disclosure only needs to teach or fairly suggest **one** of the alternatives." (emphasis added). Page 9 of Board Decision. On Rehearing, the Board maintained that (a) the fifth program instructions (as it was phrased before this Amendment) could be construed to cover the alternative and (b) only one test found in the prior art would satisfy the fifth program instructions,

> "Claims must be given the broadest reasonable interpretation consistent with Appellant's disclosure. …We do not agree with Appellants that the format of the claim limitation follows the Boolean logic of Not (A or B) to strictly imply not A and not B. While prefacing the alternative language of the claims by a negative can cause all the factors recited therein to be considered, we find that such a construction of the claim limitation would be too narrow. As discussed in the original Opinion, under the broadest reasonable interpretation approach, we conclude that the plain meaning of the recited limitation requires that the packet bet not a known exploit, or not a portion thereof, or not network administration traffic, or not another type of traffic known to be benign. Consequently, we reiterate our initial position that the prior art needs to teach one of the alternative factors." Board's decision on Rehearing dated March 3, 2011.

The Board then stated "Suuronen's disclosure only needs to teach or fairly suggest **one** of the alternatives", and proceeded to affirm the rejection under 35 USC 103(a).

The fifth paragraphs of the pending independent claims have been amended herein to clearly recite that determination that the packet is a new, exploit candidate is based on **none** of the conditions being present. For example, claim 1 recites "the fifth program instructions are responsive to the packet not being a known exploit or portion thereof AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler, to determine that the packet is a new, exploit candidate". Therefore, the independent claims, as amended above, recite a multi-part test in the fifth program instructions and therefore, overcome the issue cited by the Board.

A claim cannot be obvious under 35 USC 103 unless (a) there is a reason that a person of ordinary skill in the art would have combined the references, and (b) all the claim elements are taught or suggested by the prior art. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438, 1443 (Fed Cir. 1991) and KSR Int'l Co. v. Teleflex, Inc., No. 04-1350 (USSC 30 April 2007).

Rejection of Claims 1, 4-5, 7 and 12 under 35 USC 103(a) based on Suuronen et al. and Amit et al.

Independent Claim 1 was rejected under 35 USC 103 based on Suuronen et al. and Amit et al. Appellants respectfully traverse this rejection, as applied to the claims as amended herein, based on the following.

Claim 1 recites in part, "fifth program instructions, responsive to the packet not being a known exploit, AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate".

Suuronen et al. disclose a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams (packets called the "first type" in Suuronen et al.), which cannot be viruses and should bypass the virus scanning engine to increase throughput. The objective is to avoid the overhead and delays involved in virus screening of audio and video data streams, which need to reach their destination in real time, and are not viruses. Suuronen et al. also state that packets of the "first type" include "other real time data which cannot contain viruses are not delayed by the virus scanning engine." However, Suuronen et al. fail to disclose the second and third program instructions of claim 1 which determine if the packet is addressed to a broadcast IP address of a network or network administrative traffic. Suuronen et al. fail to disclose the fifth program instructions which are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate.

Also, Suuronen et al. do not teach or suggest identification of new, exploit candidates as specified in the fifth program instructions of claim 1. Rather, Suuronen et al. merely determine which packets should be passed to (or conversely bypass) a virus scanning engine "with virus detection criteria specified by virus detection database 24." See Suuronen et al. Paragraph 0021. Thus, Suuronen et al. determine if the packets contain a known virus **signature**. If a packet passes through the virus scanning engine of Suuronen, this means that the packet is presumed not to be a virus. The virus scanning engine of Suuronen et al. does not attempt to identify new, exploit candidates that do not exist in the virus detection database.

Amit et al. do not fill the many gaps of Suuronen et al. Amit et al. are concerned with simulating a web browser by monitoring TCP/IP data packets routed through a communication line and filtering relevant requests and responses relating to a given IP address. These requests and responses are analyzed and sorted according to their type and content. Based on the analysis, a probe terminal identifies all relevant data transactions relating to the navigation process of the given terminal. The probe terminal activates a virtual browser simulating the processing of identified data transactions to create navigation presentations similar to the real navigation as seen by the user of the given terminal.

Amit et al. disclose a method of tracking a network communication line by a network probe terminal simulating a browser activity of a terminal comprising the steps of accessing the network communication line, tracing TCP/IP data packets routed through the communication line, selecting TCP/IP data packets relating to a given IP address, selecting from the identified data packets current requests for new connections, selecting from the identified data packets current web page components indicating new addressees, dividing the new navigation components into two categories, embedded objects or frames, hyperlinks, dividing the original requests into original request matching true the new components, or original request failing to match any new connection components and belonging to HTTP or POST type as primary requests, original requests matching the false components as secondary requests, selecting from identified data packets, HTML data files relating to primary requests, generating virtual secondary requests according to the respective secondary responses, selecting from identified data packets responses relating to secondary virtual requests and simulating web page presentation on the terminal agent according to the respective secondary responses. See Summary of Amit et al. Paragraph 0017.

However, Amit et al. are not concerned with identifying new exploits. Amit et al. do not fill any of the foregoing gaps of Suuronen et al. Amit et al. fail to disclose the second and third program instructions of claim 1 which determine if the packet is addressed to a broadcast IP address of a network or network administrative traffic as part of a program (or system) for identifying new exploits. Thus, Amit et al. fail to disclose the fifth program instructions which are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate. Therefore, there is not a prima facie case of obviousness.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. because they address much different tasks and problems. Suuronen et al. are concerned with a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams which cannot be viruses and should bypass the virus scanning engine. Amit et al. are concerned with monitoring network traffic to simulate browser activity and thereby simulate navigation presentations similar to the real navigation as seen by the user of the terminal. See Abstract and Paragraphs 0038 of Amit et al. These are much different technologies involving different technicians, and there would be no reason to combine these two documents.

Independent claim 25 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover.

Rejection of Claim 2 under 35 USC 103(a) based on Suuronen et al. and Amit et al.

Claim 2 depends on claim 1 and recites sixth program instructions to determine if the packet is web crawler traffic. In addition, the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler traffic, to determine that the packet is a new, exploit candidate. Neither Suuronen et al. nor Amit et al. teach or suggest these features of claim 2. While Suuronen et al. teach a firewall to identify "data packets which cannot contain viruses", Suuronen et al. do not teach the foregoing program instructions of claim 2. Amit et al. are concerned with simulating a web browser and do not fill this gap of Suuronen et al.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. as explained above with reference to claim 1.

Rejection of Claim 9 under 35 USC 103(a) based on Suuronen et al., Amit et al. and Grenot

Claim 9 depends on claim 1. In addition, claim 21 recites another criterion to determine whether the packet is a new, exploit candidate, i.e. whether the packet has a protocol listed in a list of protocols previously determined to be harmless broadcast traffic. This other criterion is not taught or suggested by Suuronen et al., Amit et al. and Grenot, individually or in combination.

Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot discloses that an identification signature for each data packet is calculated. Grenot also discloses that "each packet is subjected to a classification operation 44. Criteria for classification are typically those that are conventionally retained to identify flows between networks and sub-networks (such as IP network sub-addresses), flows between end equipment (such as IP addresses), flows between applications (such as IP addresses and UDP/TCP transport addresses), etc. Each packet is then identified by combining all or part of the elements: class, date signature." Column 6 lines 26-34. However, Grenot does not disclose or even suggest a program for determining new, exploit candidates. Rather, Grenot is concerned with measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot does not disclose any algorithm for determining new, exploit candidates. Grenot does not disclose the algorithm of claim 1 for determining new, exploit candidates. Even though Grenot identifies various IP addresses associated with a packet, Grenot does not perform the program operations of claim 1 to determine new, exploit candidates. Grenot fails to disclose program instructions of claim 9 which determine whether a packet is a new, exploit candidate based on whether the packet is a known exploit, addressed to a broadcast IP address of the network or network administration traffic or has a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and Grenot and there would be no reason to combine Suuronen et al. with Amit et al. and Grenot because they address much different tasks and problems. Suuronen et al. are concerned with a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams which cannot be viruses and should bypass the virus scanning engine. Amit et al. are concerned with monitoring network traffic to simulate browser activity and thereby simulate navigation presentations similar to the real navigation as seen by the user of the terminal. See Abstract and Paragraphs 0038 of Amit et al. Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. These are much different technologies involving different technicians, and there would be no reason to combine these three documents.

Rejection of Claims 3, 8, 10-11 and 24 under 35 USC 103(a) based on Suuronen et al., Amit et al. and Grenot

Claims 3, 8 and 10-11 depend on claim 1 and therefore distinguish over Suuronen et al. and Amit et al. for the same reasons that claim 1 distinguishes thereover. Claim 24 depends on claim 21 and therefore distinguishes over Suuronen et al. and Amit et al. for the same reasons that claim 21 distinguishes thereover. Grenot does not fill the foregoing gaps of Suuronen et al. and Amit et al. relative to base claims 1 and 21.

Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot discloses that an identification signature for each data packet is calculated. Grenot also discloses that "each packet is subjected to a classification operation 44. Criteria for classification are typically those that are conventionally retained to identify flows between networks and sub-networks (such as IP network sub-addresses), flows between end equipment (such as IP addresses), flows between applications (such as IP addresses and UDP/TCP transport addresses), etc. Each packet is then identified by combining all or part of the elements: class, date signature." Column 6 lines 26-34. However, Grenot does not disclose or even suggest a program for determining new, exploit candidates. Rather, Grenot is concerned with measuring transfer durations and loss rates of data packets in high volume telecommunications networks. Grenot does not disclose any algorithm for determining new, exploit candidates. Grenot does not disclose the algorithm of claim 1 for determining new, exploit candidates. Even though Grenot identifies various IP addresses associated with a packet, Grenot does not perform the program operations of claim 1 to determine new, exploit candidates. Grenot fail to disclose the fifth program instructions of claim 1, i.e. "the fifth program instructions are responsive to the packet not being a known exploit or portion thereof AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler, to determine that the packet is a new, exploit candidate".

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and Grenot and there would be no reason to combine Suuronen et al. with Amit et al. and Grenot because they address much different tasks and problems. Suuronen et al. are concerned with a virus scanning engine, and a bypass/screening system to identify certain packets such as audio and video data streams which cannot be viruses and should bypass the virus scanning engine. Amit et al. are concerned with monitoring network traffic to simulate browser activity and thereby simulate navigation presentations similar to the real navigation as seen by the user of the terminal. See Abstract and Paragraphs 0038 of Amit et al. Grenot teaches a system and method for measuring transfer durations and loss rates of data packets in high volume telecommunications networks. These are much different technologies involving different technicians, and there would be no reason to combine these three documents.

Rejection of Claim 21 under 35 USC 103(a)
based on Suuronen et al. and Amit et al.

Independent claim 21 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. In addition, claim 21 recites another criterion to determine whether the packet is a new, exploit candidate, i.e. whether the packet has a protocol listed in a list of protocols previously determined to be harmless broadcast traffic. This other criterion is not taught or suggested by Suuronen et al. and Amit et al. Moreover, this other criterion is not taught or suggested by Grenot and there would be no reason to combine Suuronen et al. with Amit et al. and Grenot as explained above with reference to dependent claim 9.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. as explained above with reference to claim 1.

Rejection of Claim 22 under 35 USC 103(a)
based on Suuronen et al. and Amit et al.

Claim 22 depends on claim 21 and recites sixth program instructions to determine if the packet is web crawler traffic. In addition, the fifth program instructions are responsive to the packet not being a known exploit or portion thereof AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being web crawler, to determine that the packet is a new, exploit candidate. Neither Suuronen et al. nor Amit et al. teach or suggest these features of claim 22. While Suuronen et al. teach a firewall to identify "data packets which cannot contain viruses", Suuronen et al. do not teach the foregoing program instructions of claim 22. Amit et al. do not fill this gap either.

Moreover, it would not have been obvious to combine Suuronen et al. with Amit et al. and there would be no reason to combine Suuronen et al. with Amit et al. as explained above with reference to claim 1.

Rejection of Claim 6 under 35 USC 103(a)
based on Suuronen et al., Amit et al. and Hasegawa et al.

Claim 6 depends on claim 1 and therefore distinguishes over Suuronen et al. and Amit et al. for the same reasons that claim 1 distinguishes thereover. Hasegawa et al. disclose a network traffic monitoring system comprising a plurality of active traffic monitors each tapping a physical line on a network and analyzing traffic, and a central manager collecting data from the plurality of active traffic monitors. Hasegawa et al. do not fill the gaps of Suuronen et al. and Amit et al. noted above in relation to claim 1.

Rejection of Claim 23 under 35 USC 103(a)
based on Suuronen et al., Amit et al. and Hasegawa et al.

Claim 23 depends on claim 21 and therefore distinguishes over Suuronen et al. and Amit et al. for the same reasons that claim 21 distinguishes thereover. Hasegawa et al. disclose a network traffic monitoring system comprising a plurality of active traffic monitors each tapping a physical line on a network and analyzing traffic, and a central manager collecting data from the plurality of active traffic monitors. Hasegawa et al. do not fill the gaps of Suuronen et al. and Amit et al. noted above in relation to claim 21.

Based on the foregoing, Appellants request allowance of the present patent application as amended above.

Respectfully submitted,

Dated: April 29, 2011
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz
Arthur J. Samodovitz
Reg. No. 31,297